LINEAR CHARACTERS OF SL_2 OVER DEDEKIND DOMAINS

HATICE BOYLAN AND NILS-PETER SKORUPPA

Abstract. For an important class of arithmetic Dedekind domains $\mathfrak{o}$ including the ring of integers of not totally complex number fields, we describe explicitly the group of linear characters of $\mathrm{SL}(2,\mathfrak{o})$. For this, we determine, for arbitrary Dedekind domains $\mathfrak{o}$, the group of linear characters of $\mathrm{SL}(2,\mathfrak{o})$ whose kernel is a congruence subgroup.

1. Statement of results and discussion

It is well-known that the group of linear characters of $\mathrm{SL}(2,\mathbb{Z})$ is cyclic of order 12. The literature contains various formulas for the linear characters of $\mathrm{SL}(2,\mathbb{Z})$. These are either produced as a byproduct in the theory of modular forms as consequence of the transformation law of the Dedekind η-function under $\mathrm{SL}(2,\mathbb{Z})$ [Ded77], [Ded30], or else show up in the purely group theoretical calculation of character tables of the groups $G_N := \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. These groups contain nontrivial linear characters only for $N = 2, 3, 4$. For these N, the groups of linear characters of G_N are generated by the characters ε_N, respectively, which are given by the formulas

$$
\begin{aligned}
\varepsilon_2(A) &= e^{\frac{2\pi i}{2}(\mathrm{t}(A)+1)\,\{A\}_2},\\
\varepsilon_3(A) &= e^{\frac{2\pi i}{3}\,\mathrm{t}(A)\,\{A\}_3},\\
\varepsilon_4(A) &= s(A)\,e^{\frac{2\pi i}{4}(\mathrm{t}(A)+1)\,\{A\}_4}.
\end{aligned}
\tag{1}
$$

Here $\mathrm{t}(A)$ denotes the trace of A. Moreover, for $A = \left[\begin{smallmatrix} * & b \\ c & * \end{smallmatrix}\right]$ in G_N, we use $\{A\}_N = 0$ if $A = \pm 1$ or $N = 4$ and $A \equiv 1 \bmod 2$, we use $\{A\}_N = 1$ if $\mathrm{t}(A)^2 \neq 4$, and otherwise we have $\{A\}_N = u$, where $u = c$ if c is a unit, and $u = -b$ otherwise. Finally, $s(A) = -1$ if A can be written in the form $1+2\left[\begin{smallmatrix} a & b \\ c & * \end{smallmatrix}\right]$ such that $a+b+c$ is odd, and $s(A) = 1$ otherwise. It is easy to see that the functions ε_N are class functions (see the remark at the end of Section 3), but it is more difficult to see that they are indeed linear characters. We were not able to find any reference which

2010 *Mathematics Subject Classification.* Primary 20H05, Secondary 11F41.

Parts of this article were prepared during the participation of the authors in the *Arithmetic Statistics* program (2011) at the *Mathematical Sciences Research Institute, Berkeley*, which was supported by the National Science Foundation of USA (Award Number 0757627).

describes the characters of G_N by simple formulas similar to (1). We refer to Section 3 for a deduction of these formulas. Note that ε_N has order N. The group of linear characters of $\mathrm{SL}(2,\mathbb{Z})$ is generated by the two characters which are obtained by composing ε_3 and ε_4 with the natural reduction maps from $\mathrm{SL}(2,\mathbb{Z})$ onto G_3 and of G_4, respectively.

Using the same procedure we can define characters for $\mathrm{SL}(2,\mathfrak{o})$ for an arbitrary ring $\mathfrak{o}$. Namely, if $\mathfrak{l}$ is an ideal such that $\mathfrak{o}/\mathfrak{l} \cong \mathbb{Z}/N\mathbb{Z}$ for some $N \in \{2,3,4\}$, we have available the nontrivial character

$$\varepsilon_{\mathfrak{l}} := \varepsilon_N \circ \mathrm{red}_{\mathfrak{l}}$$

of $\mathrm{SL}(2,\mathfrak{o})$, where $\mathrm{red}_{\mathfrak{l}}$ is the natural map from $\mathrm{SL}(2,\mathfrak{o})$ to G_N which maps a matrix A to the matrix which is obtained by replacing each entry x of A by the residue class modulo N of any integer y such that $x \equiv y \bmod \mathfrak{l}$.

By the very construction, $\varepsilon_{\mathfrak{l}}$ is trivial on matrices A which are congruent to 1 modulo $\mathfrak{l}$. Recall that a subgroup of $\mathrm{SL}(2,\mathfrak{o})$ is called *congruence subgroup* if it contains the kernel $\Gamma(\mathfrak{l})$ of the natural map $\mathrm{SL}(2,\mathfrak{o}) \to \mathrm{SL}(2,\mathfrak{o}/\mathfrak{l})$ for some nonzero ideal $\mathfrak{l}$. For an integral domain $\mathfrak{o}$, the intersection of two congruence subgroups is again a congruence subgroup since the intersection of $\Gamma(\mathfrak{l})$ and $\Gamma(\mathfrak{m})$ contains $\Gamma(\mathfrak{l}\mathfrak{m})$, and $\mathfrak{l}\mathfrak{m}$ is nonzero if $\mathfrak{l}$ and $\mathfrak{m}$ are so. Accordingly, for an integral domain $\mathfrak{o}$, the linear characters of $\mathrm{SL}(2,\mathfrak{o})$ whose kernel is a congruence subgroup form a subgroup of the group of all linear characters of $\mathrm{SL}(2,\mathfrak{o})$, which we shall denote by $\mathrm{SL}(2,\mathfrak{o})^\sharp$.

As we shall show in Section 2, the construction in the penultimate paragraph is, for Dedekind domains $\mathfrak{o}$, the only way to obtain linear characters whose kernel is a congruence subgroup. However, there is another character, which we have to consider. The prime ideals of Dedekind domains $\mathfrak{o}$ which have residue field $\mathbb{F}_2$[1] fall into two classes, namely, those prime ideals $\mathfrak{q}$ such that $\mathfrak{q}$ divides 2 but $\mathfrak{q}^2$ does not, and those prime ideals $\mathfrak{r}$ such that $\mathfrak{r}^2$ divides 2. In the former case $\mathfrak{o}/\mathfrak{q}^2 \cong \mathbb{Z}/4\mathbb{Z}$, whereas in the latter case $\mathfrak{o}/\mathfrak{r}^2 \cong R := \mathbb{F}_2[t]/(t^2)$. Note that we can write any element A in $\mathrm{SL}(2,R)$ uniquely in the form $A = A_0(1+\alpha B)$, where A_0 is in $\mathrm{SL}(2,\mathbb{F}_2)$ and B an element of the additive group of matrices over $\mathbb{F}_2$ whose traces equal zero, and where we use $\alpha = t + (t^2)$. We define a linear character ε_4' on $\mathrm{SL}(2,R)$ by setting

$$\varepsilon_4'(A) = (-1)^{a+b+c} \qquad \left(A = A_0\left(1+\alpha\left[\begin{smallmatrix} a & b \\ c & * \end{smallmatrix}\right]\right)\right). \tag{2}$$

(For the proof that this defines indeed a character see Section 3.) Again, if $\mathfrak{l}$ is an ideal of the ring $\mathfrak{o}$ such that $\mathfrak{o}/\mathfrak{l} \cong R$ we set

$$\varepsilon_{\mathfrak{l}}' := \varepsilon_4' \circ \mathrm{red}_{\mathfrak{l}},$$

[1] We use $\mathbb{F}_p$ for the finite field with p elements.

where $\mathrm{red}_{\mathfrak{l}}$ denotes the natural map from $\mathrm{SL}(2,\mathfrak{o})$ to $\mathrm{SL}(2,R)$ which is obtained by reducing the entries of a matrix over $\mathfrak{o}$ modulo $\mathfrak{l}$ and applying the unique isomorphism from $\mathfrak{o}/\mathfrak{l}$ onto R (the uniqueness of such an isomorphism follows form the fact that R has no nontrivial automorphisms).

Theorem 1. *Let $\mathfrak{o}$ be a Dedekind domain*[2]*. Then the group $\mathrm{SL}(2,\mathfrak{o})^\sharp$ of linear characters of $\mathrm{SL}(2,\mathfrak{o})$ whose kernel is a congruence subgroup equals the direct product*

$$\prod_{\mathfrak{p}}\langle\varepsilon_{\mathfrak{p}}\rangle\times\prod_{\mathfrak{q}\|2}\langle\varepsilon_{\mathfrak{q}^2}\rangle\times\prod_{\mathfrak{r}^2|2}\big(\langle\varepsilon_{\mathfrak{r}}\rangle\times\langle\varepsilon'_{\mathfrak{r}^2}\rangle\big),\tag{3}$$

where $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ run through all prime ideals of $\mathfrak{o}$ such that $\mathfrak{o}/\mathfrak{p}=\mathbb{F}_3$, $\mathfrak{o}/\mathfrak{q}=\mathbb{F}_2$, $\mathfrak{o}/\mathfrak{r}=\mathbb{F}_2$, and such that $\mathfrak{q}^2$ does not divide 2 and $\mathfrak{r}^2$ divides 2.

The assumption of the theorem excludes fields. However, if $\mathfrak{o}$ is a field then $\mathrm{SL}(2,\mathfrak{o})$ does anyway not possess nontrivial linear characters unless $\mathfrak{o}=\mathbb{F}_2$ or $\mathfrak{o}=\mathbb{F}_3$ (see the remark at the end of Section 2).

For a Dedekind domain $\mathfrak{o}$, the number of ideals $\mathfrak{p}$ such that $\mathfrak{o}/\mathfrak{p}=\mathbb{F}_p$, for a given prime number p, is always finite (since every such ideal divides the ideal generated by all elements of the form a^p-a, which is not zero if $\mathfrak{o}$ is infinite). Thus, for a Dedekind domain $\mathfrak{o}$, the group $\mathrm{SL}(2,\mathfrak{o})^\sharp$ is always finite. This holds not true for an arbitrary integral domain. The ring $\mathbb{F}_2^{\mathbb{Z}}$ of all maps from $\mathbb{Z}$ to $\mathbb{F}_2$ with argumentwise addition and multiplication provides a counterexample. Here, for any integer n, the map $A\mapsto\varepsilon_{3\mathbb{Z}}\big(A(n)\big)$ yields an element of $\mathrm{SL}(2,\mathbb{F}_2^{\mathbb{Z}})^\sharp$.

There is another interesting consequence of Theorem 1. Namely, if, for an arbitrary ring $\mathfrak{o}$, a subgroup Γ of $\mathrm{SL}(2,\mathfrak{o})$ contains the commutator subgroup of $\mathrm{SL}(2,\mathfrak{o})$ then, for every A which is not in Γ there exists a linear character χ whose kernel is Γ but such that $\chi(A)\neq 1$[3]. If $\mathfrak{o}$ is a Dedekind domain, and if Γ is a congruence subgroup, then χ equals one of the characters in $\mathrm{SL}(2,\mathfrak{o})^\sharp$. Accordingly, A is not contained in the intersection $B(\mathfrak{o})$ of the kernels of the linear characters in $\mathrm{SL}(2,\mathfrak{o})^\sharp$. In other words, Γ contains $B(\mathfrak{o})$. But $B(\mathfrak{o})$ is of finite index in $\mathrm{SL}(2,\mathfrak{o})$. Hence we have

Corollary 1. *Let $\mathfrak{o}$ be a Dedekind domain. The number of congruence subgroups of $\mathrm{SL}(2,\mathfrak{o})$ containing the commutator subgroup $K(\mathfrak{o})$ is finite.*

In particular, we see that the commutator subgroup of $\mathrm{SL}(2,\mathfrak{o})$, for any Dedekind domain $\mathfrak{o}$, possesses a congruence closure, namely the

[2] In this note fields are not considered as Dedekind domains.

[3] Since Γ contains the commutator subgroup, it is normal. Any maximal extension of a linear character ψ on $\langle A\Gamma\rangle$ with $\psi(A\Gamma)\neq 1$ to a subgroup of $G:=\mathrm{SL}(2,\mathfrak{o})/\Gamma$, whose existence is ensured by Zorn's lemma, has by a standard argument G as its domain, and therefore provides such a character.

subgroup $B(\mathfrak{o})$. This is surprising since the index of the commutator subgroup in $\mathrm{SL}(2,\mathfrak{o})$ is not necessarily finite (see below).

If K is a global field, i.e. an algebraic number field or a function field in one variable over a finite field, then, for every finite set of places of K comprising the archimedean ones, the ring $\mathfrak{o}_S$ of S-integers is a Dedekind domain. The ring $\mathfrak{o}_S$ consists of all elements of K whose valuation at a place v of K is ≥ 0 unless v is in S. If $\mathrm{card}(S) \geq 2$ then the abelianization $\mathrm{SL}(2,\mathfrak{o}_S)^{\mathrm{ab}}$ of $\mathrm{SL}(2,\mathfrak{o}_S)$ is finite ([Ser70, Thm. 3, Cor.]). Moreover, if at least one place of S is real or nonarchimedean then all subgroups of finite index in $\mathrm{SL}(2,\mathfrak{o}_S)$ are congruence subgroups ([Ser70, Thm. 2, Cor. 3]). Hence, as a consequence of Theorem 1 we obtain

Theorem 2. *Assume that $\mathfrak{o}$ is the ring of S-integers of a global field, where $\mathrm{card}(S) \geq 2$ and S contains at least a real or a nonarchimedean place. Then the group of* all *linear characters of* $\mathrm{SL}(2,\mathfrak{o})$ *coincides with* $\mathrm{SL}(2,\mathfrak{o})^\sharp$*, i.e. it equals the group* (3).

Note, that the theorem implies, for function fields of one variable over a finite field $\mathbb{F}$ and every finite set S of at least two places, that $\mathrm{SL}(2,\mathfrak{o}_S)$ has no nontrivial character if the characteristic of $\mathbb{F}$ is different from 2 and 3.

The assumptions of Theorem 2 apply, in particular, to the ring of integers of a number field different from $\mathbb{Q}$ which is not totally complex.

Corollary 2. *Let $\mathfrak{o}$ be the ring of integers of an algebraic number field with at least one real embedding. Then the group of* all *linear characters of* $\mathrm{SL}(2,\mathfrak{o})$ *coincides with the group* $\mathrm{SL}(2,\mathfrak{o})^\sharp$*, i.e. it equals the group* (3)*. In particular, the order of the abelianized group* $\mathrm{SL}(2,\mathfrak{o})^{\mathrm{ab}}$ *equals* 3^a4^b*, where a and b denote the number of prime ideals of degree* 1 *over* 3 *and over* 2*, respectively.*

In Section 4 we present some numerics concerning the abelianized groups $\mathrm{SL}(2,\mathfrak{o})$ for rings of integers of number fields.

For imaginary quadratic fields the situation can be very different. Indeed, let $\mathfrak{o}$ equal the ring of integers in $\mathbb{Q}(\sqrt{-7})$. The abelianized group $\mathrm{SL}(2,\mathfrak{o})^{\mathrm{ab}}$ is isomorphic to $\mathbb{Z}\oplus\mathbb{Z}_4$ (see [Coh68, p. 162]), hence the group of linear characters equals $\mathrm{S}^1 \times \mathbb{Z}_4$, where S^1 is the subgroup of complex numbers of modulus 1. In particular, here the group $\mathrm{SL}(2,\mathfrak{o})$ possesses infinitely many characters of finite order. This example shows that, even for a Dedekind ring, the group $\mathrm{SL}(2,\mathfrak{o})^\sharp$ can be smaller than the torsion subgroup of the group of linear characters.

We do not know whether the corollary holds true in general for totally complex number fields with at least 2 complex places. We have many examples where it holds true (see Section 4), but do not know of any counterexample.

As already mentioned we did not find any reference for the formulas (1). Though one can verify them easily by a case by case analysis of conjugacy classes in G_N using a character table (see e.g. [GAP08]), we decided to give a deduction from scratch in Section 3. The proof of Theorem 1 is given in Section 2.

2. Proof of Theorem 1

For an arbitrary ring $\mathfrak{o}$, we use $\mathfrak{o}^*$ for its group of units. We set

$$T(a) := \begin{bmatrix} 1 & a \\ & 1 \end{bmatrix} \quad (a \text{ in } \mathfrak{o}), \quad E(a) := \begin{bmatrix} a & \\ & a^{-1} \end{bmatrix} \quad (a \text{ in } \mathfrak{o}^*), \quad S = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}.$$

Recall that the matrices $T(a)$ and their transposes are called *elementary matrices*. Note also, that $\mathrm{SL}(2,\mathfrak{o})$ is generated by elementary matrices if and only if it is generated by the matrices $T(a)$ and S (since $S = \begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix}\begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & \\ a & 1 \end{bmatrix} = ST(-a)S^{-1}$).

For a linear character χ of $\mathrm{SL}(2,\mathfrak{o})$, the map $a \mapsto \chi(T(a))$ defines a linear character ξ of the (additive) group $\mathfrak{o}$. The set of a in $\mathfrak{o}$ such that $\xi(ab) = 1$ for all b in $\mathfrak{o}$ forms an $\mathfrak{o}$-ideal $\mathfrak{a}$, which we call the *annihilator of* χ. For a nonzero ideal $\mathfrak{l}$, we say that χ has *level* $\mathfrak{l}$ if χ is trivial on the subgroup $\Gamma(\mathfrak{l})$ of all matrices in $\mathrm{SL}(2,\mathfrak{o})$ which are congruent modulo $\mathfrak{l}$ to the unit matrix. Clearly, if χ has level $\mathfrak{l}$ then $\mathfrak{l}$ contains the annihilator.

Lemma 1. *Let $\mathfrak{o}$ be an arbitrary ring. Then the $\mathfrak{o}$-ideal generated by the elements $u^2 - 1$, where u runs through the group of units of $\mathfrak{o}$, is contained in the annihilator of any linear character of* $\mathrm{SL}(2,\mathfrak{o})$.

Proof. The lemma is an immediate consequence of the formula

$$T(bu^2) = E(u)T(b)E(1/u),$$

valid for all b in $\mathfrak{o}$ and all units u. $\square$

Lemma 2. *Assume that* $\mathrm{SL}(2,\mathfrak{o})$ *is generated by elementary matrices. Let K denote the commutator subgroup of* $\mathrm{SL}(2,\mathfrak{o})$. *Then the application*

$$\mathfrak{o} \to \mathrm{SL}(2,\mathfrak{o})^{\mathrm{ab}} := \mathrm{SL}(2,\mathfrak{o})/K \quad a \mapsto T(a)K \tag{4}$$

defines a surjective group homomorphism.

Proof. The lemma follows from the fact that $\big(ST(1)\big)^3 = S^2$, so that $SK = T(1)^{-3}K$, from which we recognize that $\mathrm{SL}(2,\mathfrak{o})^{\mathrm{ab}}$ is generated by the elements $T(a)K$. $\square$

Lemma 3. *Let $n \geq 1$ and let $\mathfrak{p}^n$ be a prime ideal power in the Dedekind domain $\mathfrak{o}$. Suppose that $u^2 = 1$ for every u in $(\mathfrak{o}/\mathfrak{p}^n)^*$. Then one of the following statements holds true:*

1. *$n = 1$ and $\mathfrak{o}/\mathfrak{p}^n = \mathbb{F}_2$ or $\mathfrak{o}/\mathfrak{p}^n = \mathbb{F}_3$.*
2. *$n = 2$ or $n = 3$, $\mathfrak{p}$ divides 2 but $\mathfrak{p}^2$ does not, and $\mathfrak{o}/\mathfrak{p}^n = \mathbb{Z}/2^n\mathbb{Z}$.*
3. *$n = 2$, $\mathfrak{p}^2$ divides 2, and $\mathfrak{o}/\mathfrak{p}^n = \mathbb{F}_2[t]/(t^2)$.*

Proof. By assumption $U := (\mathfrak{o}/\mathfrak{p})^*$ has exponent ≤ 2. Since $\mathfrak{p}$ is maximal, $F := \mathfrak{o}/\mathfrak{p}$ is a field. Hence every finite subgroup of U is cyclic. It follows that U has order 1, and hence $F = \mathbb{F}_2$, or else U has order 2, and hence $F = \mathbb{F}_3$.

Suppose $n \geq 2$. Then $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_2$, since in the case of $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_3$ the group of units of $\mathfrak{o}/\mathfrak{p}^2$ has order 6. If $\mathfrak{p}^2$ does not divide 2, then $\mathfrak{o}/\mathfrak{p}^n = \mathbb{Z}/2^n\mathbb{Z}$, and since $\mathbb{Z}/16\mathbb{Z}$ has elementary divisors 2 and 4, we conclude $n \leq 3$.

Suppose finally that $\mathfrak{p}^2$ divides 2. Let α denote any element in $\mathfrak{p}$ which is not contained in $\mathfrak{p}^2$. Then $(1+\alpha)^2 = 1 + 2\alpha + \alpha^2 \not\equiv 1 \bmod \mathfrak{p}^3$, from which we conclude $n = 2$. But $\mathfrak{o}/\mathfrak{p}^2 = \mathbb{F}_2[\alpha + \mathfrak{p}^2] = \mathbb{F}_2[t]/(t^2)$. ☐

Proof of Theorem 1. For proving Theorem 1 recall that $\mathfrak{o}$ is now a Dedekind domain. Suppose that χ is a nontrivial linear character of $\mathrm{SL}(2, \mathfrak{o})$ whose kernel contains $\Gamma(\mathfrak{l})$ for some nonzero ideal $\mathfrak{l}$. The homomorphism $\mathrm{SL}(2, \mathfrak{o}) \to \mathrm{SL}(2, \mathfrak{o}/\mathfrak{l})$ induced by the canonical map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{l}$ is surjective ([Bas64, cor. 5.2]). We may therefore consider χ as a character of $\mathrm{SL}(2, \mathfrak{o}/\mathfrak{l})$. The canonical map

$$\mathrm{SL}(2, \mathfrak{o}/\mathfrak{l}) \to \prod_{\mathfrak{p}^l \| \mathfrak{l}} \mathrm{SL}(2, \mathfrak{o}/\mathfrak{p}^l)$$

induced from the Chinese remainder theorem, where $\mathfrak{p}^l$ runs through the prime ideal powers dividing $\mathfrak{l}$, is an isomorphism of groups. Accordingly χ factors into a product of characters $\chi_\mathfrak{p}$, where $\chi_\mathfrak{p}$ has level $\mathfrak{p}^l$. For the proof of Theorem 1 we may therefore assume that χ is a nontrivial character of $\mathrm{SL}(2, \mathfrak{o})$ with level $\mathfrak{l} = \mathfrak{p}^l$ for some prime ideal $\mathfrak{p}$. It is clear that the annihilator $\mathfrak{a}$ of χ contains $\mathfrak{l}$, hence is of the form $\mathfrak{p}^n$. We claim that the group of units $(\mathfrak{o}/\mathfrak{a})^*$ has exponent ≤ 2.

Indeed, let u be a unit of $\mathfrak{o}/\mathfrak{a}$. The canonical map $x + \mathfrak{l} \mapsto x + \mathfrak{a}$ from $\mathfrak{o}/\mathfrak{l}$ to $\mathfrak{o}/\mathfrak{a}$ induces a surjective homomorphism of the group of units (since the group of units is formed by the residue classes which are relatively prime to $\mathfrak{p}$). We therefore find a preimage u' of u in $\big(\mathfrak{o}/\mathfrak{l}\big)^*$. But then, by Lemma 1, $u'^2 - 1$ is contained in the annihilator of the character $\widetilde{\chi}(a + \mathfrak{l}) = \chi(a)$ of $\mathrm{SL}(2, \mathfrak{o}/\mathfrak{l})$, which equals $\mathfrak{a}/\mathfrak{l}$. We conclude $u^2 = 1$.

Since χ is nontrivial, the annihilator $\mathfrak{a} = \mathfrak{p}^n$ is different from $\mathfrak{o}$, i.e. we have $n \geq 1$. Indeed, if the annihilator of χ equaled $\mathfrak{o}$, the annihilator of $\widetilde{\chi}$ would be $\mathfrak{o}/\mathfrak{l}$. But Lemma 2, applied to $\mathfrak{o}/\mathfrak{l}$ instead of $\mathfrak{o}$, would imply that $\widetilde{\chi}$ is trivial. For applying Lemma 2 we need that $\mathrm{SL}(2, \mathfrak{o}/\mathfrak{l})$ is generated by elementary matrices, which is, in fact, well-known [Bas68, Ch. 5, Cor. 9.3]. However, for a quotient $\mathfrak{o}/\mathfrak{l}$ of a Dedekind domain by a nonzero ideal $\mathfrak{l}$ this can more easily be proven directly as follows. By using the Chinese remainder theorem, we may assume that $\mathfrak{l}$ equals a prime ideal power $\mathfrak{p}^l$. But then $\mathfrak{o}/\mathfrak{l}$ is a local ring. Hence, if $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is a matrix in $\mathrm{SL}(2, \mathfrak{o}/\mathfrak{l})$,

then either c is a unit (and then $A = T(a/c)ST(dc)E(c)$), or a is unit (and then $A = ST(-c/a)ST(ba)E(-a)$). For a unit u, we have $E(-u) = ST(1/u)ST(u)ST(1/u)$.

We can therefore apply Lemma 3 to deduce that one of the three cases (1) to (3) apply to $\mathfrak{o}/\mathfrak{a} = \mathfrak{o}/\mathfrak{p}^n$. But this suffices to compute $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^l)^{\mathrm{ab}}$. Namely, since $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^l)$ admits the nontrivial character $\widetilde{\chi}$, it possesses a nontrivial character whose annihilator is minimal. Without loss of generality we can assume that $\widetilde{\chi}$ assumes minimal annihilator. The map (4) of Lemma 2 factors then through a surjection

$$\mathfrak{o}/\mathfrak{p}^n \to \mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^l)^{\mathrm{ab}}.$$

According to cases (1) to (3) of Lemma 3 we deduce that $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^l)^{\mathrm{ab}}$ has order ≤ 2 or ≤ 3 in case (1), and has order ≤ 4 in case (2) and (3). In fact, the lemma implies only the bound 8 in case (2) if $n = 3$, but we know already from the structure of $\mathrm{SL}(2,\mathbb{Z})^{\mathrm{ab}}$ that $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^3) \cong \mathrm{SL}(2,\mathbb{Z}/8\mathbb{Z})$ admits exactly four characters. The existence of the characters $\varepsilon_{\mathfrak{p}}$, $\varepsilon_{\mathfrak{p}^2}$ and $\varepsilon'_{\mathfrak{p}^2}$ shows that we have indeed equality in all three cases, and that any linear character of $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{p}^l)$ is a power or product of these characters.

That the subgroups occurring in (3) form a direct product is easily seen by evaluating a product of elements of these groups on matrices which are congruent to the unit matrix modulo all the primes occurring in the products except for one, and using that, for $\mathfrak{r}^2|2$, we have $\mathrm{SL}(2,\mathfrak{o}/\mathfrak{r}^2) \cong \mathrm{SL}(2,\mathbb{F}_2[t]/(t^2)) = \mathrm{SL}(2,\mathbb{F}_2) \ltimes \Gamma((t)/(t^2))$ (see (6)) and that $\varepsilon_{\mathfrak{r}}$ and $\varepsilon'_{\mathfrak{r}^2}$ vanish on one of these factors, respectively. This proves Theorem 1. □

Let $\mathfrak{o}$ be a field such that $\mathrm{SL}(2,\mathfrak{o})$ possesses a nontrivial character. The annihilator of this character, not being equal to $\mathfrak{o}$ since the character is nontrivial, is the zero ideal. Hence, by Lemma 1, $u^2 = 1$ for all nonzero elements in $\mathfrak{o}$. Since every subgroup of $\mathfrak{o}$ is cyclic, we conclude that $\mathfrak{o}^*$ has order 1 or 2, i.e. that $\mathfrak{o}$ equals $\mathbb{F}_2$ or $\mathbb{F}_3$.

3. The linear characters of $\mathrm{SL}(2,\mathbb{Z})$ and $\mathrm{SL}(2,\mathbb{F}_2[t]/(t^2))$

In this section we shall prove the formulas (1) and (2). Recall, first of all, that that $\mathrm{SL}(2,\mathbb{Z})$ is generated by $T = \left[\begin{smallmatrix}1&1\\&1\end{smallmatrix}\right]$ and $S = \left[\begin{smallmatrix}&-1\\1&\end{smallmatrix}\right]$. If χ is a linear character of $\mathrm{SL}(2,\mathbb{Z})$ which maps T to, say ζ, then χ maps S to ζ^{-3} (since $(ST)^3 = S^2$), from which it follows that $\zeta^{12} = 1$ (since $S^4 = 1$) and that $\mathrm{SL}(2,\mathbb{Z})$ possesses at most 12 linear characters. In fact, since the characters ε_3 and ε_4 define characters (as we shall show in a moment) which have order 3 and 4, respectively, we conclude that the abelianization of $\mathrm{SL}(2,\mathbb{Z})$ has exact order 12.

The formulas (1) result all from the remarkable decompositions

$$G_N = \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}) = \langle T\rangle \ltimes K_N \qquad (N = 2,3,4), \tag{5}$$

where K_2 and K_3 are the 3-Sylow and 2-Sylow subgroups of G_2 and G_3, respectively, and where K_4 is the subgroup of G_4 generated by the elements of order 3 in G_4. Mapping T to -1, $e^{2\pi i/3}$, i for $N = 2, 3, 4$, respectively defines accordingly a character of G_N, which is in fact, as we shall see in a moment, the character ε_N. Note that in each case G_N does not possess any other character than powers of ε_N, since, as we saw, the group $\mathrm{SL}(2, \mathbb{Z})$ possesses only 12 characters. In particular, K_N is the commutator subgroup of G_N.

Next, we prove for each N the existence of the decomposition (5) and verify the claimed formula (1) for ε_N.

The nontrivial linear character ε_2 of G_2 corresponds to the signature map on permutations when we identify G_2 with the symmetric group S_3 via its natural action on the nonzero column vectors in $(\mathbb{Z}/2\mathbb{Z})^3$. Thus $\varepsilon_2(A) = -1$ if A corresponds to a transposition, i.e. if A has order 2, and $\varepsilon_2(A) = +1$ otherwise. Note that A has order 2 if and only if its characteristic polynomial $x^2 - tx + 1$ equals $x^2 - 1$, i.e. if $t = \mathrm{t}(A) = 0$. The formula (1) for ε_2 is now obvious, as is the decomposition (5), where K_2 corresponds to the alternating subgroup under any isomorphism $\mathrm{SL}(2, \mathbb{F}_2) \cong S_3$.

We note that G_3 has 24 elements and exactly one 2-Sylow subgroup K_3, which is then normal. In fact, G_3 has exactly 8 elements whose order divides 8, which must then form the 2-Sylow subgroup of G_3. The decomposition (5) becomes now evident.

Note that K_3 consists of those matrices A which are either equal to ± 1 or whose trace t equals 0. Namely, for any $A \neq \pm 1$ of order dividing 8, its characteristic polynomial $x^2 - tx + 1$ must divide the polynomial $x^8 - 1 = (x + 1)(x - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1)$, hence equals $x^2 + 1$. Accordingly, we find, for any $A = \left[\begin{smallmatrix} * & b \\ c & * \end{smallmatrix}\right]$ in G_3, that $\varepsilon_3(A) = e^{2\pi i n/3}$, where n is chosen so that $T^{-n}A$ equals ± 1 or has trace $t = 0$, i.e., where $n = -tb$ if $c = 0$ or $n = tc$ otherwise. From this formula (1) can be verified.

Finally, the group G_4 has 48 elements. It has 8 elements of order 3. We show, first of all, that the subgroup K_4 generated by these elements has order 12. Note that this already implies the decomposition (5) since K_4 does then not contain any power of T except the unit matrix (since the normal subgroup generated by T or T^2 contains more than 4 elements), and since K_4 is normal (by its very definition). Clearly, K_4 is contained in the inverse image K_2' of the 3-Sylow subgroup K_2 of G_2 under the natural reduction map. But $K_2' = \langle G \rangle \ltimes \Gamma(2)$, where G is any fixed element of order 3 (since K_2' has order 24 and the kernel $\Gamma(2)$ of the reduction map modulo 2 has order 8). The application $X \mapsto 1 + 2X$ defines an isomorphism from the (additive) group L of matrices over $\mathbb{F}_2$ with trace 0 onto $\Gamma(2)$. There is exactly one subgroup of L which is invariant under conjugation with elements in G_2, namely the subgroup L_0 of elements $X = \left[\begin{smallmatrix} a & b \\ c & * \end{smallmatrix}\right]$ in M such that $a + b + c = 0$.

Accordingly, we obtain a linear character s of K_2' by setting $s(A_0 + 2A_1) = 1$ if $A_0^{-1}A_1$ is in L_0, and setting $s(A_0 + 2A_1) = -1$ otherwise. The kernel of s contains all 8 elements of order 3 and has order 12, hence coincides with the subgroup generated by the elements of order 3. We remark that K_4 is isomorphic to the alternating group A_4 (via the action of conjugacy on its four 3-Sylow subgroups).

Note that an element has order 3 if and only if its trace t equals -1 (since, for a matrix A with trace t and characteristic polynomial $\chi_A = x^2 - tx + 1$, we have $x^3 - 1 = (x+t)\,\chi_A + (t+1)\big((t-1)x - 1\big)$). Thus, for any $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with trace t, we have $\varepsilon_4(A) = i^n$, where n is chosen such that $T^{-n}A$ is in K_4. We choose $n = (t+1)c$ if c is odd (so that $T^{-n}A$ has trace -1), $n = b + 2$ if $A = \left[\begin{smallmatrix} * & * \\ 2 & 1 \end{smallmatrix}\right]$, (so that $T^{-n}A = 1 + 2\left[\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right]$), $n = -b$ if $A = \left[\begin{smallmatrix} * & * \\ 2 & -1 \end{smallmatrix}\right]$ (so that $T^{-n}A = 1 + 2\left[\begin{smallmatrix} 1 & \\ 1 & 1 \end{smallmatrix}\right]$), $n = b$ if if $A = \left[\begin{smallmatrix} 1 & b \\ & 1 \end{smallmatrix}\right]$ (so that $T^{-n}A = 1$), and $n = 2 - b$ if $A = \left[\begin{smallmatrix} -1 & b \\ & -1 \end{smallmatrix}\right]$ (so that $T^{-n}A = 1 + 2\left[\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right]$). We leave it to the reader to check that i^n coincides in all cases with the right hand side of formula (1).

We remark that the quantities $\{A\}_N$ occurring in formula (1) depend only on the conjugacy class of A. For this note that the application $A \mapsto f_A = cx^2 + (d-a)xy - by^2$ maps conjugate matrices to G_N-equivalent quadratic forms (more precisely, one has $f_{BAB^{-1}}(x, y) = f_A\big((x, y)B\big)$ for B in G_N), and that $\{A\}_N = I(f_A)$ for a map I which depends only on the G_N-equivalence classes of forms. More specifically, $I(Q) = 0$ if $Q = 0$ or $N = 4$ and $Q \equiv 0 \bmod 2$, $I(Q) = 1$ if $\mathrm{disc}(Q) \neq 0$, and $I(Q) = Q(1, 0)$ is a unit and $I(Q) = -Q(0, 1)$ otherwise.

Finally, we determine the linear characters of $\mathrm{SL}(2, R)$ where $R = \mathbb{F}_2[t]/(t^2)$. Let $\alpha = t + (t^2)$. Note, first of all, that we have an isomorphism of groups $M \to \Gamma(\alpha)$, $X \mapsto 1 + \alpha X$, where M is the additive subgroup of matrices over $\mathbb{F}_2$ whose traces equal 0. The group M has eight elements. Any matrix in $\mathrm{SL}(2, R)$ can be written in the form $A + \alpha B$, where A and B are matrices with entries in $\mathbb{F}_2$. The application $A + \alpha B \mapsto A$ yields an exact sequence

$$1 \to \Gamma(\alpha) \to \mathrm{SL}(2, R) \to \mathrm{SL}(2, \mathbb{F}_2) \to 1.$$

Since $\mathrm{SL}(2, \mathbb{F}_2)$ is a subgroup of $\mathrm{SL}(2, R)$ this sequence splits, and we conclude that

$$\mathrm{SL}(2, R) = \mathrm{SL}(2, \mathbb{F}_2) \ltimes \Gamma(\alpha). \tag{6}$$

The group $\Gamma(\alpha)$ has 7 nontrivial characters, of which only one is invariant under conjugation with $\mathrm{SL}(2, \mathbb{F}_2)$, This is the character given by $\varepsilon_4'(1 + \alpha\left[\begin{smallmatrix} a & b \\ c & * \end{smallmatrix}\right]) = (-1)^{a+b+c}$, which can then be continued to a character of $\mathrm{SL}(2, R)$ by setting $\varepsilon_4'(A + \alpha B) = \varepsilon_4'(1 + \alpha A^{-1}B)$. The other nontrivial character of $\mathrm{SL}(2, R)$ is $\varepsilon_{(\alpha)}$.

4. Statistics for number fields

We append three tables. The first one shows, for each pair of integers (n, r) $(2 \leq n \leq 7,\ r)$ the first number field K of degree n and with exactly r real embeddings for which $\mathrm{SL}(2, \mathbb{Z}_K)$ admit a nontrivial linear character ($\mathbb{Z}_K$ denoting the ring of integers of K). For generating these data we used the Bordeaux tables of number fields [cntg07], which list for each pair (n, r) the first few hundred thousands of number fields K having the given signature ordered by the absolute value of their discriminant D_K. The calculations were done using [S$^+$11]. According to Corollary 2 we had, to search for each number fields in the Bordeaux tables for the existence of prime ideals of degree 1 over 2 or over 3. For the totally complex fields of degree ≥ 3, this would not suffice to make sure that there are no additional non-congruence characters (for degree $n = 2$ the first field $\mathbb{Q}(\sqrt{-3})$ admits already 3 linear characters). Here we proceeded as follows. Once we found, for a given degree n, the first field K admitting a nontrivial congruence character, we checked that, for each of the finitely many fields L with $|D_L| < |D_K|$, the ideal generated by $u^2 - 1$ $(u \in \mathbb{Z}_L^*)$ is 1. Since, for not imaginary quadratic K, the group $\mathrm{SL}(2, \mathbb{Z}_K)$ is generated by elementary matrices [Vas72] and by the following proposition we can deduce that $\mathrm{SL}(2, \mathbb{Z}_K)$ does not possess any nontrivial character.

Proposition 1. *Assume that the ring $\mathfrak{o}$ is generated by elementary matrices. Then $\mathrm{SL}(2, \mathfrak{o})^{\mathrm{ab}}$ is trivial if the $\mathfrak{o}$-ideal $\mathfrak{b}$ generated by $u^2 - 1$ $(u \in \mathfrak{o}^*)$ equals $\mathfrak{o}$.*

Proof. By Lemma 2, we have a surjective map $\mathfrak{o} \to \mathrm{SL}(2, \mathfrak{o})^{\mathrm{ab}}$, which, by Lemma 1, factors through a surjective map

$$\mathfrak{o}/\mathfrak{b} \to \mathrm{SL}(2, \mathfrak{o})^{\mathrm{ab}}. \tag{7}$$

From this the proposition is obvious. □

Similarly, we computed the second table, which lists the first fields K of given degree n and number of real embeddings r, for which $\mathrm{SL}(2, \mathbb{Z}_K)$ admits the maximal possible number of linear characters. For degree ≥ 4 (with exception of $n = 4$, $r = 0$) we did not find any such fields in the range of the Bordeaux tables. For $n = 2$, $r = 0$ we put a question mark since $\mathbb{Q}(\sqrt{-23})$ is the first imaginary quadratic field such that $\mathrm{SL}(2, \mathbb{Z}_K)$ possesses exactly 144 congruence characters, whereas for the order of the abelianized group as well as for the groups $\mathrm{SL}(2, \mathbb{Z}_L)^{\mathrm{ab}}$ for arbitrary imaginary quadratic number fields L we do not have any information (except for some special fields L which were treated in the literature, see e.g. [Coh68]). For $n = 4$, $r = 0$ we computed for all fields L with $D_L < 940033$ the ideals $\mathfrak{b}_L$ generated by the elements $u^2 - 1$ $(u \in \mathbb{Z}_L^*)$, and verified that $\mathfrak{b}_L$ decomposes into a product of pairwise different prime ideals over 3 and squares of pairwise different

prime ideals over 2. Again from the surjectivity of the map (7) we can deduce that $\mathrm{SL}(2,\mathbb{Z}_K)$ admits only congruence characters as linear characters.

TABLE 1. First number fields K with nontrivial $\mathrm{SL}(2,\mathbb{Z}_K)^{\mathrm{ab}}$.

n	r	D_K	equation	$\#\mathrm{SL}(2,\mathbb{Z}_K)^{\mathrm{ab}}$
2	0	-3	x^2-x+1	3
2	2	8	x^2-2	4
3	1	-31	x^3+x-1	3
3	3	81	x^3-3x-1	3
4	0	189	x^4-x^3+2x+1	3
4	2	-491	$x^4-x^3-x^2+3x-1$	3
4	4	1957	x^4-4x^2-x+1	3
5	1	3089	x^5-x^3+2x-1	3
5	3	-9439	$x^5-x^4-x^3+x^2-2x+1$	3
5	5	36497	$x^5-2x^4-3x^3+5x^2+x-1$	3
6	0	-19683	x^6-x^3+1	3
6	2	63909	x^6+2x^4-x-1	3
6	4	-233003	$x^6-3x^4-3x^3+4x^2+x-1$	3
6	6	1259712	$x^6-6x^4+9x^2-3$	3
7	1	-435247	$x^7-x^6-x^5+3x^4-x^3-x^2+2x+1$	3
7	3	1602761	$x^7-2x^6+2x^5+x^4-3x^3+5x^2-4x+1$	3
7	5	-6930439	$x^7-x^6-3x^5+5x^4-2x^3-3x^2+3x+1$	3
7	7	25164057	$x^7-2x^6-5x^5+9x^4+7x^3-10x^2-2x+1$	3

TABLE 2. First number fields K with $\#\mathrm{SL}(2,\mathbb{Z}_K)^{\mathrm{ab}} = 12^{[K:\mathbb{Q}]}$

n	r	D_K	equation
2	0	? -23	x^2-x+6
2	2	73	x^2-x-18
3	1	-10079	$x^3+11x-36$
3	3	49681	$x^3-37x-12$
4	0	940033	$x^4-x^3+44x^2+4x+384$

TABLE 3. First totally real abelian number fields K unramified outside a prime l with $\#\mathrm{SL}(2,\mathbb{Z}_K)^{\mathrm{ab}} = 12^{[K:\mathbb{Q}]}$

l	equation
73	x^2-x-18
307	$x^3-x^2-102x+216$
577	$x^4-x^3-216x^2+36x+1296$
3221	$x^5-x^4-1288x^3-17780x^2-30432x+285696$
3889	$x^6-x^5-1620x^4+360x^3+174960x^2-11664x-1259712$
5531	$x^7-x^6-2370x^5+21108x^4+746040x^3-2927424x^2$ $-46637056x+70303744$
6529	$x^8-x^7-2856x^6+26830x^5+2014493x^4-23400945x^3$ $-374849822x^2+2921535140x+29083370664$

Finally, in Table 3 we listed, for each degree $n \leq 8$, the smallest prime l such that the lth cyclotomic field contains a totally real number field K such that $\mathrm{SL}(2, \mathbb{Z}_K)$ admits the theoretically maximal possible number of linear characters. An equation for K is given in the second column, respectively. It is straightforward to show that as primitive element of these fields one may take $\gamma_l = \sum_{x \bmod l} e^{2\pi i x^n/l}$. However, the corresponding minimal polynomial has quite huge coefficients, so we applied to it in Sage the Pari/GP function `gp('polred(...)')` to find an equation with smaller coefficients.

In [BS11] the interested reader can find the results of all our computations, in particular the order of $\mathrm{SL}(2, \mathbb{Z}_K)^{\mathrm{ab}}$ for all (not totally complex) number fields in the range of the Bordeaux tables.

References

[Bas64] H. Bass. K-theory and stable algebra. *Inst. Hautes Études Sci. Publ. Math.*, (22):5–60, 1964.

[Bas68] Hyman Bass. *Algebraic K-theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[BS11] Hatice Boylan and Nils-Peter Skoruppa. Linear characters of $\mathrm{SL}(2, \mathbb{Z}_K)$. `http://data.countnumber.de`, 2011.

[cntg07] Bordeaux computational number theory group. The number field tables. `http://pari.math.u-bordeaux.fr`, 2007.

[Coh68] P. M. Cohn. A presentation of SL_2 for Euclidean imaginary quadratic number fields. *Mathematika*, 15:156–163, 1968.

[Ded77] Richard Dedekind. Schreiben an Herrn Borchardt über die Theorie der elliptischen Modul-Functionen. *J. Reine Angew. Math.*, 83:265–292, 1877.

[Ded30] Richard Dedekind. Erläuterungen zu zwei Fragmenten von Riemann. In Robert Fricke, Emmy Noether, and Öystein Ore, editors, *Richard Dedekind, Gesammelte mathematische Werke*, volume 1, pages 159–173. Friedr. Vieweg & Sohn Akt.-Ges., Braunschweig, 1930.

[GAP08] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[S$^+$11] W. A. Stein et al. *Sage Mathematics Software (Version 4.6.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[Ser70] Jean-Pierre Serre. Le problème des groupes de congruence pour SL2. *Ann. of Math. (2)*, 92:489–527, 1970.

[Vas72] L. N. Vaseršteĭn. The group SL_2 over Dedekind rings of arithmetic type. *Mat. Sb. (N.S.)*, 89(131):313–322, 351, 1972.

RWTH Aachen and Universität Siegen
hatice.boylan@gmail.com

Universität Siegen
nils.skoruppa@gmail.com